University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: Risikostyring – Offshoresikkerhet	**Spring semester, 2012** **Open** / ~~Restricted access~~
Writer: Monphen Toungsetwut	…… (Writer's signature)
Faculty supervisor: Eirik Bjorheim Abrahamsen **External supervisor(s):** None	
Title of thesis: Analytical Methods for Risk Assessment and reduction of the uncertainty	
Credits (ECTS): 30 study points	
Key words: Risk, FMECA, FTA, HAZOP, Uncertainty, Bayesians Network, Sensitivity Analysis	Pages: ……48…… + enclosure: ……....7…….…… Stavanger, 12 June 2012

Abstract

Risk is in involved in all activities especially in oil and gas industries. It is involved from the day one the project has started. Risk during the exploration phase, the chance that you found only dry wells the company may lose a fortune or risk during planning and design phase, the wrong design has been selected the project will face problems and gradually with maturity of the project.

This paper will talk about risk with focusing during planning and design phase in oil and gas industries. Get to know and understand analysis methods will assist in choosing a right method(s) for the job. A combination set of analysis methods will fulfill the objective of analyst process. A study case of three phase separator will be used throughout the paper.

In chapter 3 Analytical methods, three well known and most use methods – Failure Mode Effect and Criticality Analysis (FMECA), Fault Tree Analysis (FTA) and Hazard and Operability Study (HAZOP) – will be present in this paper with pros and cons, strengths and weaknesses with suggestions for improvement, what the result of the analysis are, how it can assist you in decision making process and help in select right method according to the purpose of your analysis.

Uncertainty is an important factor that we must consider during perform an analysis. Therefore chapter 4 Dealing with uncertainties will discuss about two methods – Bayesians Network and Sensitivity Analysis - that analyse should perform in order to reduce any uncertainty that involved in the primary analyst. The final risk analysis result from chapter 3 will be analysis once again with Bayesians Network and Sensitivity Analysis in order to reduce the uncertainties that may involve.

Acknowledgements

First and foremost, I would like to thank to my supervisor of this thesis, Associate Professor Eirik Bjorheim Abrahamsen at the University of Stavanger, for the encouragement, valuable guidance and advice

Anne Sissel Svensen, administrator of Science and Technology faculty, for the advice and support throughout my study program at University of Stavanger.

I am also grateful to all my friends at the University of Stavanger and outside, who support and contributed in different ways. Especially to Hermanto Ang, Jahedul Islam, Marcelo Ernesto Guaranì Cortéz for suggestions and brainstorm sessions we have during the master thesis period.

My beloved family and friends in Thailand for the support, strengths, best wishes they always give and always there for me.

Last but not least, Marco Antonio Céspedes Guzmán for his love, patient, support and understanding he gives.

Table of Contents

Table of figures

Table of tables

1. Introduction

Every action, every activity and every business is inherited risk. Risk cannot be eliminated but can always reduce and prevent.

We may classify risk into two big categories. First economic risk which included all risk related with cost. Reliability is strongly related with economic risk due to variance in availability of the system and/or component reflex the revenue and cost during the down-time of the system. Therefore decision that been made during conceptual and design phase is also give a big impact to the whole project. We may select the cheapest equipment that available in the market, but most of this case will end up with higher maintenance cost and followed with less system availability. Second safety risk which included all risk related with health and safety of people and environment. Safety analysis must be conducted in order to avoid and prevent incident.

There are numbers of methods to analyse risk and they has different weaknesses and strengths. Risk cannot be analyzed by a single method. A combination of methods is a must to ensure that all the possible risk has been consider and minimized below the risk acceptance criteria.

How to ensure that the method(s) we select are best choice and for the correct purpose? What are the advantages and disadvantages of each method? What is the information you will get from the analysis? In what aspect those analysis results will do to the project? We can answer these questions once we know the method well, and select the right one based on the objective of analyse process.

The traditional risk analysis based on traditional probability and calculated from P(A|K) – the probability of event A occurs given K as background knowledge or background information – without consider the uncertainty in those background information. Many of the accident in the past occurred because the uncertainties in background information has not ignored, undiscovered and not well managed.

Analyse can choose to analyst risk with traditional approach and try to reduce uncertainty of the final analysis' result or to adapt new theory to reduce the uncertainties during analysis process.

2. Definition and abbreviation

2.1 Definition

Availability The probability that a system is not failed or undergoing a repair action when it needs to be used[1]

Down time The amount of time a repairable unit is not operation. This can be due to being in a failed state, administrative delay, waiting for replacement parts to be shipped or undergoing active repair[1]

Failure The termination of the ability of an item to perform a required function[2]

NOTE - After failure the item has a fault. "Failure" is an event, as distinguished from a "fault", which is a state (prEN 13306)

Failure mechanism Physical, chemical or other processes which lead or have led to failure (prEN 13306)[2]

Failure rate Number of failures of an item in a given time interval divided by the time interval (prEN 13306)[2]

NOTE 1 - This value is an approximation.
NOTE 2 - In some cases time can be replaced by units of use.(In most cases 1/MTTF can be used as the predictor for the failure rate, i.e. the average number of failures per unit of time in the long run if the units are replaced by an identical unit at failure. Failure rate can be based on operational or calendar time.)

Failure mode The observed manner of failure (ISO 14224)[2]

Inspection Activity carried out periodically and used to assess the progress of damage in a component[2]

NOTE 1 - Inspection can be by means of technical instruments (e.g. NDT) or as visual examination.
NOTE 2 - prEN 13306 has been deviated from in order to apply to the most common use of the term "inspection" in the oil and gas industry, which relates inspection and inspection management to the activity of checking the conformity of the equipment by NDT instruments or visual examination at regular intervals.

Maintenance Combination of all technical, administrative and managerial actions, including supervision actions, during the life cycle of an item intended to retain it in, or restore it to, a state in which it can perform the required function (prEN 13306)[2]

Reliability	The probability of components, parts and systems to perform their required functions for a desired period of time without failure in specified environments with a desired confidence[1]
Probability	A quantitative description of the possible likelihood of a particular event. Probability is conventionally expressed on a scale from 0 to 1, or 0% to 100%, with an unlikely event having a probability close to 0, and very common event having a probability close to 1[1]
Up time	The amount of time a repairable unit is operating per design[1]

2.2 Abbreviation

CAPEX Capital Expenditure

FMECA Failure Mode Effect and Criticality Analysis

FTA Fault Tree Analysis

HAZOP Hazard and Operability Study

MDT Mean Maintenance Down Time

MTBF Mean Time between Failures

MTTF Mean Time to Failure

MTTR Mean Time to Repair

OPEX Operational Expenditure

3. Analytical methods

There are many methods or model that can be use to conduct risk analysis. Each method has its own strengths and weaknesses. Analyst should be able to select the most-fit method with regard to the aim and purpose of the analysis and tailored made to the analysis objective, operational phase of the selected infrastructure.

Even thought different method has been rise, but the main purpose of conducting risk analysis is to give decision-making support in both selecting of solutions and measures.

Risk can be described by (A, C, U, P, K), when A is equal to events, C equal consequences or outcome of an event A, U equal uncertainty in associated with both A and C, P is the probability the events A and consequences C and given the knowledge or background knowledge as K.[3]

Further in this chapter we will describe how the methods link to risk that described with (A, C, U, P, K) especially uncertainty in risk analysis.

3.1 Failure Mode Effect and Criticality Analysis

Failure Mode Effect and Criticality Analysis method is a systematic analysis method which developed by the U.S. Military. The first guideline was Military Procedure MIL-P-1692 dated November 9, 1949[4]. It's often called FMECA or FMEA. The different between FMECA and FMEA is in FMECA has added detail regarding criticality or severity of the failure which is an important factor to create "Risk Matrix" for future use.

> *"FMECA is quantitative method of reliability analysis which involves a fault modes and effects analysis together with a consideration of the probability of failure modes, their consequence and ranking of effects and the seriousness of the faults (BS 3811)"*

FMECA explore and identifies the effects, probability, failure rate, criticality, consequences, how to avoid, how to detect and how to mitigate the effects of the failure or malfunctions of each individual components in an observed sub-system in detail level. It is widely conducted during conceptual and design phase since it gives information such as probability, failure rate (the numbers can be found from many source such as knowledge-base (K), historical date or OREDA – Offshore Reliability Database) and effect of the failure (how badly it effect to the sub-system and to the whole system) which can assist us pre-select the best alternative or revise design if needed (see Figure 1).

By conducting FMECA we can ensure that all potential failure has been considered and proper actions have been made to eliminate these known potential failures before they occur.

The boundary of the system or subsystem must be verified so that you will only consider components in the system without consider any effect it might have from external source. This is one of the weaknesses of FMECA method which we will discuss later in this chapter.

3.1.1 FMECA with project life cycle

FMECA in conceptual and design phase

In the early phase as conceptual and design phase gives the most impact on equipment reliability. As the design matures, it becomes more difficult to alter. Unfortunately, the time, cost, and resources required to correct a problem increase as well.[5]

By consider component in sub-system and with all information you have after performed FMECA, we can compare all options we have and select the best choice. The question is "what factors determine the best?", "Shall we select from the cheapest provider?", "Shall we select the alternative that most reliable?", "Shall we select the option with the cheapest maintenance cost?", "Shall we select the option which gives lowest criticality?" Those are the questions we all face when it comes to decision making.

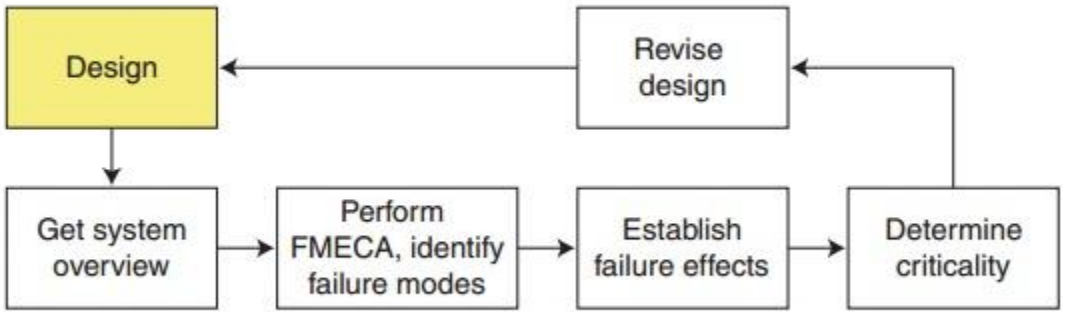


FIGURE 1 FMECA IN DESIGN PHASE[4]

With my own opinion quality always come with the price. Means if you want a good piece of equipment or part you would have to pay more. The figure below (see Figure 2) illustrates a draft example the relation between CAPEX and OPEX with regard to reliability of the system and it proves my simple opinion.

There are two options that the team needs to select. Option A's CAPEX is lower than option B. In option B the company must invest more in project startup (CAPEX) such as equipment cost, installing, construction but supplier will benefit more from this different.

Let's look at the overall project cost, option A's overall project cost is higher than option B. The OPEX cost is the cost during operation such as maintenance, repair, inspection routine and including the lost of profit during shutdown (if any in case of downtime). The different is the company's benefit since the more reliability the equipment is the less downtime and more availability we will get.

We can see that by selecting the more reliable equipment is a win-win situation to both party (supplier and the company). Supplier increasing benefit by provide higher reliability products to customer, definitely the company will have to pay more for those products. Company increasing benefit in total project cost because the high reliability products give higher availability in production phase and lower maintenance cost.

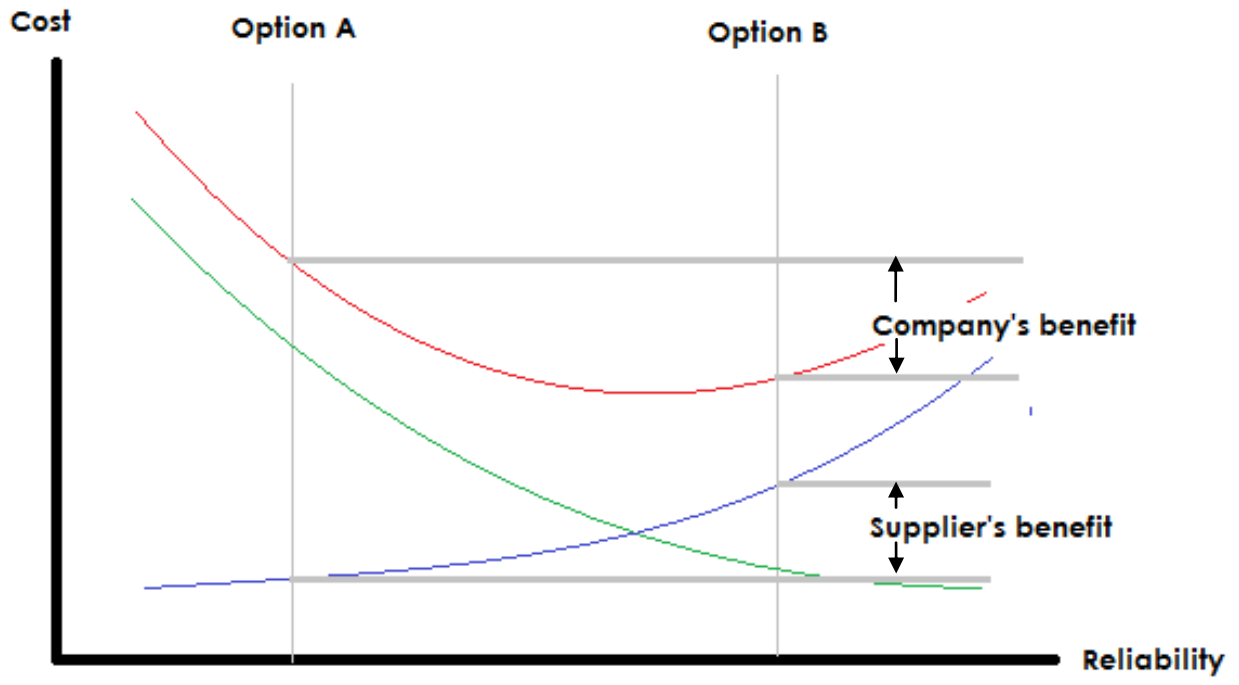


FIGURE 2 SELECTING OPTIONS

NB! Blue line, green line and red line represent CAPEX, OPEX and Overall project cost respectively.

FMECA in production phase

Information such as MTTF, MTBF, MTTR, and MDT can be included in FMECA report for future use during production phase. It gives overview of all components for example expected failure date, life time of the component, and required time during maintenance.

To plan maintenance schedule gives many advantage during production phase. Here are some examples:

- Allow changing of the component before the component failure (referred from MTTF). Must take extra closer look at critical component
- Allow inspection of the component before it worn out and lead to component failure (referred from MTTF)
- Allow maintenance routine to schedule during planned temporary shutdown
- Increase availability – no downtime = higher availability
- Increase reliability – routine inspection to ensure that component is in good condition
- Allow routine maintenance to extend component's life time

For extended use of FMECA, we can link information from FMECA to internal database which I will give example later in this chapter.

3.1.2 FMECA process

Since FMECA will be conducted to one sub-system at the time, we need to verify which sub-system we will start to observe. Verify the boundary of the observed system. Gather the team to conduct FMECA. The team should consist of expert from different expertise area to ensure that different point of view will be given during the analysis process. The following step shall be performed:

1. *Define an observe system boundaries* – identify which part is to be included which part is not

2. *Define expected performance or the expected function of the system* – since failure of a component is including when the component not in fully function or degrade operation. For example the valve should seal a pipe 100%, if there is some leakage that's mean the valve is fail to function as it should

3. *Define operational and environmental condition* – operational and environmental condition can be storage capacity, at specific pressure and temperature, and weather. Those gives effect to the system and should take into account that FMECA is performed under these constrains and what are the consequences when we brake those constrains

4. *Prepare FMECA worksheet* – FMECA can be categorized into 3 main type[4]

    a. Design FMECA is carried out to eliminate failure during equipment design, taking into account all type of failures
    b. Process FMECA is focused on problems stemming from how the equipment is manufactured, maintained or operated
    c. System FMECA looks for potential problems and bottlenecks in larger processes, such as entire production line

    Different type of FMECA requires or prefers different information. Therefore there is no concrete FMECA worksheet, it is depend on which information fit and can assists decision making.

    Design FMECA may need information such as criticality, failure rate, consequences of the failure that assist design and concept selection
    Process FMECA may need information such as MTTF, MTBF that use in maintenance planning program
    System FMECA may need information such as potential failure mode, potential effect on the system in global.

    We shall keep in mind that we should keep it simple, add only useful information else the worksheet will look too complex and difficult to understand

5. *Collect and list all the equipments and parts* – this information can gather from many sources such as design's drawing and specification. It is important to ensure that all the parts in the system is listed

6. *Collect information from previous or similar designs from internal and external source* – information such as possible cause of each failure mode, consequences, probability, and how to detect the failure
7. *Prioritize criticality* – prioritize and identify criticality of each failure mode and propose risk reducing measure by start from the highest risk item first

8. *Agree and suggest actions* – The team agrees and suggests proper actions to mitigate the risk and proper actions in case of failure occur.

3.1.3 Pros and cons

Pros	Cons
➢ Allow feasibility study of development options[6] ➢ Design optimization ➢ Improve reliability ➢ Understanding the causes of failure that lead to the highest risks ➢ Understanding the failure mechanisms ➢ Identifying and prioritizing mitigating measure (spot the most important aspects and focus for revision to minimize those risk first) ➢ Focusing and effective test procedures (useful input for validate testing, validate each component whether it's in functional mode) ➢ Learning about failures without experiencing them ➢ Higher reliability in service ➢ Shorter development times[6] ➢ Reduction in CAPEX and OPEX[6] ➢ Help in decision making, pre-selection process ➢ Provide basic maintenance planning[7] ➢ Criticality category can be categorized based on many different perspectives. From operation perspective, the most critical is when production shut-down. From HSE perspective, the most critical can vary from large pollution to fatality (see Table 1 and Table 2)	➢ Does not consider effect(s) from external source ➢ Easy to forget failure which cause from human error[8] ➢ The worksheet can be too complex or complicate when numbers of information added ➢ Time consuming[8]

SPE-96335[9] has described benefits of using FMECA in a new technology application, such as:

- Better understanding of the key reliability issues to put the operator in a stronger position to make well informed decisions about the best applications for this technology
- The focus to ensure that action plans and resources are targeted where they will provide most benefit on preventing or mitigating the critical failure modes
- A baseline for comparisons with other technology options
- A framework which can be used for future FMECA's

"A baseline for comparisons with other technology options" benefit from the paper is conformed to "help in decision making and pre-selection process" that listed in the table above. Analyst perform FMECA of all alternatives have, compare, use the analyzed data assist in decision making process and select the best alternative. The analysis can be performed before the

application is constructed. Therefore, by conduct FMECA we can surely achieve many indirect result of the analysis such as cost saving, time saving, system's deep information are recorded for further use and may use as template for a similar application or project in the future.

The paper also put a strong focus only on the critical aspect of the analysis, focus in mitigating them. However there are no concrete set of rule or concrete category for criticality or severity.

Example of severity from SEMATECH 1992 standard

TABLE 1 SEMATECH SEVERITY RANKING CRITERIA[5]

Rank	**Description**
1–2	Failure is of such minor nature that the customer (internal or external) will probably not detect the failure.
3–5	Failure will result in slight customer annoyance and/or slight deterioration of part or system performance.
6–7	Failure will result in customer dissatisfaction and annoyance and/or deterioration of part or system performance.
8–9	Failure will result in high degree of customer dissatisfaction and cause non-functionality of system.
10	Failure will result in major customer dissatisfaction and cause non-system operation or non-compliance with government regulations.

Other example is from The Institution of Engineering and Technology

TABLE 2 IET SEVERITY RANKING CRITERIA[10]

Catagory	**Degree**	**Description**
I	Minor	Functional failure of part of machine or process - no potential for injury
II	Critical	Failure will probably occur without major damage to system or serious injury
III	Major	Major damage to system and/or potential serious injury to personnel
IV	Catastrophic	Failure causes complete system loss and/or potential for fatal injury

We can see that from two different sources they already have strong contrast in categorizing severity. One is focused and ranked based on the design concept, customer satisfaction and government regulations, while another one is focused and ranked based on a level of failure and it consequences.

3.1.4 Weaknesses and strengths

Weaknesses

One sub-system at the time – FMECA is performed on one sub-system at the time which makes it impossible to look at the system in the big picture. Additionally, it is difficult to read and to spot the most fragile or most critical component in the object sub-system especially if the system composed of numbers of small components.

Complex report – Since FMECA report doesn't have a concrete format, analyst can always choose to add one or more columns that he or she thinks that information can be useful and/or can assist decision making. For example analyst may add MTTF and MTBF for maintenance purpose but that information won't be necessary or useful during normal production phase. The problem is the more information you added, the more complex the report is. Best thing to do is to keep it simple and insert only important information that needed according to the project or to the level of the reader.

Time consume – To perform a good FMECA is a time consuming process, since each component must be consider with regard to the effect to (local) sub-system and the effect to (global) whole system. Information must be collected from many sources. For example failure rate can be found from OREDA, but failure cause or failure mechanism can be gathered from historical date or knowledge-base. An expert analyse can reduce analysis time tremendously by using his/her experience on components, using information from a similar project or analysis

Expensive – Once the observe system has been modified you will need to conduct FMECA all over again. Since the new component effect the whole observed system. Therefore FMECA need to performed in every changed we made during the design phase (see Figure 1)

Not for multi-problem – FMECA is conducted by looking at the failure which occurs on a single component while other components are in function. But in real practice failure can cause on more than one component at the time.

Overlook human factor – In many cases analyst tended to focus on mechanism or technical issue of the component and overlook at error that can cause from human error. Some of the system may need human assistance or to activate the system, but since those are external source that we didn't consider as a part of the observed system. The failure which cause from human

will be overlooked (see Weaknesses of FTA for more detail in how to reduce, prevent and avoid human error)

Uncertainties – It is in the nature of all predicted data, estimated data or even measured data always has uncertainty. Unfortunately uncertainty cannot be eliminated, but reduced.

As mention earlier that risk and uncertain are in every activities, same as the activity we perform during data gathering process. We cannot be 100% sure that the database or data we selected and used in analysis has no error or it is the database with 100% certain information. Every data on FMECA worksheet or report are uncertain due to it is a probability value that get from four different approaches[11]:

- Direct use of historical data
- Direct assignment or estimates
- Use of standard probability distribution
- Use of detailed modeling of phenomena and processes – fault tree (see 3.2 Fault Tree Analysis), Bayesian believe network (see 4.1 Bayesian networks) etc.

The failure rate is the data that often get from historical data by repeating the same experimental on the same component under the same condition over and over again, so called "Frequentist Probability". The uncertainty we found in this kind of probability is the error when repeating the experiment. Since it is likely impossible to set up exactly the same experiment over and over again. How large the number of experiment should be? How can we ensure that the experiment has been set up correctly under the designed or specific condition? There might be some error on measuring equipment, while the data is recorded, while the data is transfer from one to another, and during interpret of the data itself. Those are some source of uncertainty of measured data and are ignored in classical probability theory. Therefore, analyse should select and perform the same analysis with different database to double check or cross checking for the final result.

Another approach is probability that obtain by using background knowledge of experts or K in Risk description that mention earlier in Chapter 3 Analytical methods. This type of probability called Subjective Probability (will be discuss later on in 4.1 Bayesian networks). Uncertainty that involved in this type of probability is the estimate or the knowledge that come from experts. When we using such probability, we must consider uncertainties such as:

- How trust worthy the source of information – who are those experts, ones can called oneself an expert but maybe one doesn't. A common sense may be used. For example in a dice game, everyone knows that a dice has 6 alternatives. If the game offer high prize and high chance that you will win the game, we may use our common sense that the host may cheat or trick us somehow and we give our own estimate for the chance that we will win the game. In this case, we are the expert who gives out the information, but how trust worthy it will be this also related with risk attitude.

Another case is to select a source of information using as knowledge base information. An expert in electrical instrument couldn't give good information when it comes to knowledge of chemistry. It is uncertain that the source of information we selected is the best for the job.

- How accurate the source of information
- Does the source of information excepted worldwide or only apply for a particular area – in many situations the probability of a particular event to occur is vary from place to place. The probability that a boat will sink is vary tremendously from a calm lake to a rough sea.

Therefore it is also important that we consider these constrains and limits while we consider for a source of our knowledge base information, to reduce the uncertainties as low as possible.

What about the predicted data and estimate data? Those data is a result from estimate procedure, equation, average or mean value of history data.

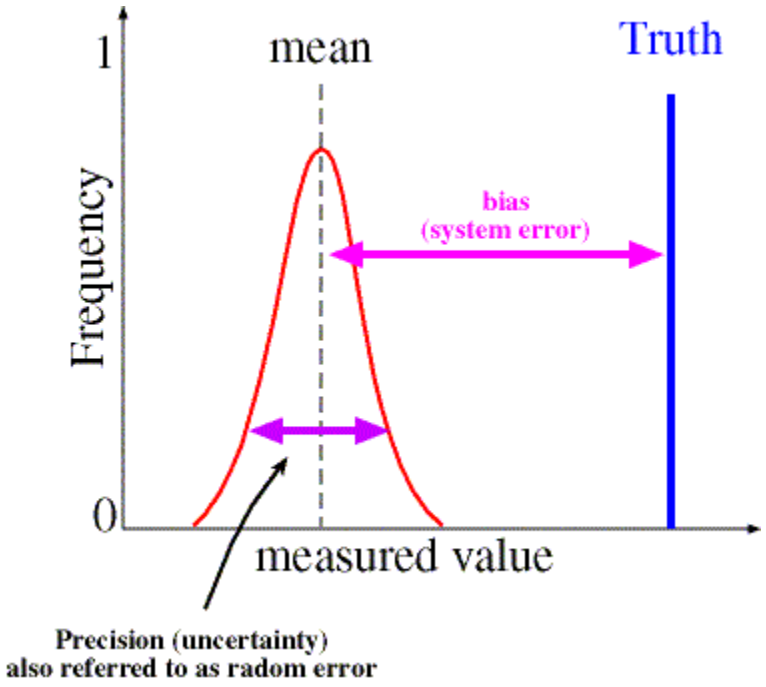


FIGURE 3 UNCERTAINTIES IN MEAN VALUE[12]

An example of uncertainty can be described from figure above (see Figure 3). Given that you have a set of measured MTTF data, you enter the data and calculate for mean value. Most of the data is covered under normal distribution, but there are a few data that plotted outside normal distribution. For example, assumed that a mean failure rate of a component in a particular failure mode - calculated from up and running 100 pieces of the same component and record the time

when it fail – is equal to 11.2 times per 10^6 working hours, and lower and upper failure rate with 90% confident interval are [2.82, 16.38], which mean there is 10% chance that the component will fail before or after 90% confident interval. Shall we overlook at those rare data?

We can play safe by design for an application or solution that reduce risk according to ALARP concept – As Low as Reasonably Practicable – which mean we need to consider the amount of money we need to invest in order to reduce the risk in our question.

Require inside knowledge from many expertise area – We may need to gather experts from difference area to ensure that all aspect and possibility is covered and considered from those who has the inside knowledge. This is cost a fortune in resources using in order to conduct an FMECA report of the observed system.

Difficult to identify the level/how large/how deep the system should be – Large system make more complicate to analyse, but on the other hand small system may too small and not useful for any future use.

Strength

Make complex system easier – The unique technique for FMECA gives an advantage for a large complex system due to FMECA need to be conducted from each sub-system. In that case you can combine FMECA report and perform root cause analysis or to investigate from the failure component. Additionally, by splitting system into small sub-system make it much easier to evaluate.

Great source for supplier selection – There are hundreds of supplier for every piece of equipment. When it comes to the decision which one we should go for, we may use information that listed and studied from FMECA report. Information such as how often it can fail, how long the component last and cost can assist us through selection process.

Assist in design selection – After the team has complete FMECA of the system, options will be considered and select the best base on information that given on FMECA report (see Figure 1)

Gives recommended action – When an actual component is fail, the recommended actions that listed in FMECA report should be called and used properly. To avoid any further failure or effect to another system that can create a larger problem.

Clear document information – Give clear information such as how to detect the failure, what to do when the failure occurred, what are the consequences.

Cost saving – The earlier you conduct FMECA, the more you save in CAPEX. Once you re-design something after the system has been build, that means the project need to fall back to the re-purchase, re-build and in worst case it will cost delayed the delivery. From the face that every project matures along with the time, therefore, the earlier you notice that re-design is needed, the more cost, time and resources saving you can make.

Assist in maintenance planning program – Knowing failure rate, MTTF and MTBF could assist you in planning a maintenance program

TABLE 3 EXAMPLE OF AN FMECA REPORT

FMECA of separator

System: Separator **Performed by:**

Subsystem: **Date:**

Function: Three-phases separator **Page:**

Description of Unit			Desciption of failure			Effect of failure		Failure Rate (per million hrs)	Criticality	Corrective action/ Risk reducing measure	Remark
Ref. No.	Function	Operational Mode	Failure mode	Failure mechanism	Detection of failure	On the subsystem	On the system function				
CV3	Separated water flow control	Open	Does not open on demand	- Not fully open - Internal failure (wear) - Receiver failure - Debris inside valve	- Increasing fluid level inside separator - Level transmitter warning system - Pressure decrease - More oil in WTS	- Close CV1	- Overfilling separator - Contamination on SI tank	1.62	Critical	- Redundant system for inlet - Routine inspection - Scheduled cleaning hydraulic line (avoid blockage)	
			Open when it is not intended	- Internal failure (wear) - Wrong signal		- None	- High hydrocarbon concentration in WTS	0.73	Critical		

3.1.5 Suggestion

For future extended use of FMECA, we can link FMECA with internal database such as supplier contact number, price of equipment (when it been purchased and current price), spare part of equipment (if any), how it manufactured, maintenance schedule to create a great information source.

Below is some examples use of such information:

- Fast and easy to find supplier contact information when we needed their assistant
- Fast and easy to evaluate, compare and select supplier when new component is needed
- Overview of spare part inventory
- Fast and easy way to access component's detail internally (how it manufacture, drawing, spec etc.)
- Assist in creating maintenance schedule, help in track and log information
- Possible to search and reuse data from similar project

3.2 Fault Tree Analysis

Fault Tree Analysis is a Top-down analysis approach that was developed in 1962 under U.S. Air Force Ballistics Systems Division at Bell Laboratories. The analyse method is to model and analyze failure processes of engineering – component failure, construction failure – and environment that relevant.

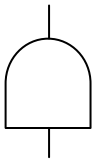
We started and focus on "Undesired event" – top event - and analyse the way down to what can cause or trigger the undesired event. All possible failure will be listed as event. This is one of many advantage of FTA since we can consider multiple events (event that can cause the undesired event).

In compare with FMECA, FTA is way faster and best-fit for trouble shooting, root cause analysis since it focus on what can contribute the undesired event without regard to all other possible failure that can lead to other event, and suitable for a complex system. This is an advantage of using fault tree to analysis a large and complex system because we do not need to analyse the whole system at once.

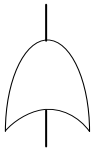
Additionally it is possible to include human error in contribution to component error that can trigger the undesired event to occur, but can only include only in qualitative analysis. The reason will be discuss later in this chapter under 3.2.2 Quantitative FTA.

In fault tree all events linked together with different gates. Two main and most important gates are "AND" gate and "OR" gate.

AND gate – the top event (output) will occur,
when all bottom events (input) occurred simultaneously.



OR gate – the top event (output) will occur,
when one or more bottom event(s) (input) occurred.



Events are described in rectangular shape. It is wise to name event with detail information rather than “fail”. Such as “valve fail”, we may describe as “valve fail to open on demand”

FTA can be done in both quantitative analysis and qualitative analysis. Probability of occurrence may be added within the event symbol for quantitative analysis. For further discussion under quantitative analysis see 3.2.2.

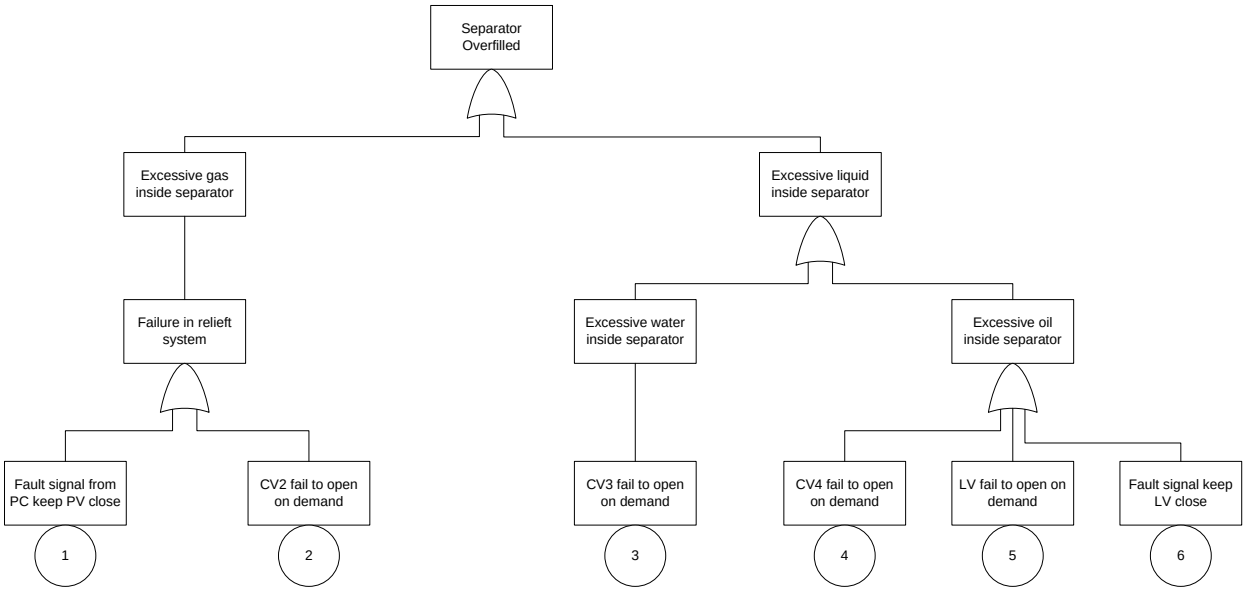


FIGURE 4 EXAMPLE OF FTA DIAGRAM

3.2.1 Qualitative FTA

Once we performed a qualitative FTA, we will get a full overview of events that caused the undesired event to occur. We may also use FT diagram as a Root Cause Analysis input data or transform FTA into Reliability Block diagram in order to easily identify redundancy of the system or cut set for further use.

Boolean value - 0 or 1 – can be assigned to each event as 0 represent system is not in function and 1 represent system is in function.

For “OR” gate of component 1 and component 2

Component 1 status	Component 2 status	System status
0	0	0
0	1	0
1	0	0
1	1	1

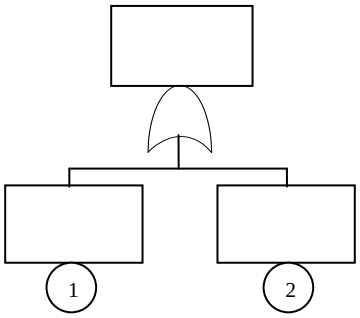


FIGURE 5 "OR" GATE

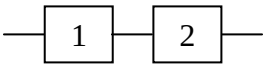


FIGURE 6 CONVERSION OF “OR” GATE (FTA TO RBD)

For “AND” gate of component 1 and component 2

Component 1 status	Component 2 status	System status
0	0	0
0	1	1
1	0	1
1	1	1

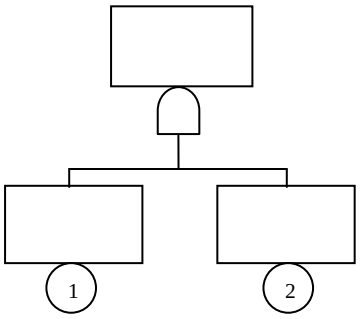


FIGURE 7 "AND" GATE

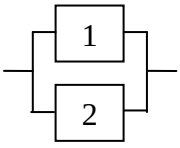


FIGURE 8 CONVERSION OF “AND” GATE (FTA TO RBD)

For quantitative analysis it is not possible to analyse a degrade system. The system can be in either function state or non-function state. Therefore a system or a component that degraded in percentage from the fully function will count as non-function state (can be vary depends on the criteria of the designer e.g. a system is in non-function state when component is at 80% functional or less).

Another possibility for degrade system is given degrade system as an undesired event in Fault tree. An example is "gas outlet to production facilities is less than 20000 cubic meter per second" (when the full capacity is 25000 cubic meter per second).

From Figure 4, we can see that all events have "OR" relationship to each other. That's mean if one of these event fail, the undesired event will occur. In other word, the system has no redundancy.

3.2.2 Quantitative FTA

For quantitative FTA, probability value has been added into each basic event and will be used in calculation for the final risk associated value. This is technically correct but contains uncertainty in the value.

Failure rate data can be collected from manufacturers' database, statistic of the component itself or from industry failure database.

Failure rate functions - $z(t)$ - is defined mathematically as:

$$z(t) = \lim_{\Delta t \to 0} \frac{1}{\Delta t} P(t < T \leq t + \Delta t | T > t)$$

Approximation:

$$z(t) \cdot \Delta t \approx P(t < T \leq t + \Delta t | T > t)$$

Both equation give approximate value which always contain uncertainty in itself. In most case, those uncertainties are forgotten or fading its importance during analysis process. Mean value are often used in calculation without regard to the uncertainty dimension.

> *"The risk analyses conducted today often have a strong focus on probabilities and expected values. Reflections associated with the uncertainty dimension and manageability are lacking"*[3]

In this paper and the study case that we will discuss later will use knowledge base information from OREDA which give information such as mean value of the failure rate per 10^6 hours, confidence interval (lower and upper limit) of the mean value and maximum likelihood of the failure rate.

$$P(\lambda_L \leq \lambda \leq \lambda_U) = 90\%$$

In additional MTTF which referred in last chapter can be calculated from:

$$MTTF = \frac{1}{\lambda}$$

When

$$\hat{\lambda} = \frac{Number\ of\ failures}{Aggregated\ time\ in\ service} = \frac{n}{\tau}$$

Example case study from Figure 4, we add failure rate information into fault tree. The case study is to analyse a possibility that a separator tank is overfilled during operation period. The "top event" or "undesired event" is "Separator Overfilled". We then brake down to possible events until we reach basic event level that can trigger the undesired event to occur. We will get Figure 9, when red value represent *mean* failure rate per 10^6 hours from OREDA and since the failure rates from OREDA are constant, therefore we can use exponential distribution represent lifetime distribution (most of electronic component have exponential distribution as lifetime distribution). The blue values represent probability of component failure after 20 years from:

$$f(t) = \lambda e^{-\lambda t}$$

When

$$t \geq 0$$

Assume that all components in the study case are non-repairable units and T is a component lifetime, t is the time that we observed.

A probability that the component will fail after time t or *F(t)* from :

$$F(t) = \int_0^t f(u)du$$

$$= \int_0^t \lambda e^{-\lambda u}\, du$$

$$= \left[-e^{-\lambda u}\right]_0^t$$

$$= -e^{-\lambda t} + 1$$

$$= 1 - e^{-\lambda t}$$

And for survivor function or *R(t)* (probability that the component is in function after time t) from:

$$R(t) = 1 - F(t)$$

$$= 1 - (1 - e^{-\lambda t})$$

$$= e^{-\lambda t}$$

From the case study "CV3 fails to open on demand" or P_4, the failure rate is equal 1.62 per 10^6 hours. We then get the probability that "CV3 fails to open on demand" after 20 years (175200 hours). (In the example I gave P_1 is the basic event on left most and P_6 is the basic event on the right most. See Figure 9)

$$F(175200) = 1 - e^{-1.62/10^6 \cdot 175200}$$

$$= 0.2471$$

For a system that all component align in series, probability or reliability that the undesired event will occur after one year can be calculate from:

$$g = 1 - h$$

$$h = \prod_{i=1}^{n} P_i$$

For a system that all component align in series, probability or reliability that the undesired event will occur after one year can be calculate from:

$$g = \prod_{i=1}^{n} q_i$$

$$h = 1 - \prod_{i=1}^{n} (1 - p_i) = \coprod_{i=1}^{n} p_i$$

When g = Unreliability of the system

h = Reliability of the system

P = Probability that system will function after one year

Therefore the reliability of the system after 20 years is equal

$$h = P_1 \cdot P_2 \cdot P_3 \cdot P_4 \cdot P_5 \cdot P_6$$

$$= 0.8955 \cdot 0.8437 \cdot 0.7529 \cdot 0.7529 \cdot 0.8647 \cdot 0.8955$$

$$= 0.3316$$

$$g = 1 - h$$

$$= 1 - 0.3316$$

$$= 0.6684$$

However, if we use lower failure rate with 90% interval, the failure rate of P_1 and P_6 = 0.03, P_2 = 0.004, P_3 and P_4 = 0.06 and P_5 = 0.03 and the probability that components are in function after 20 years are 0.9948, 0.9993, 0.9895, 0.9895, 0.9945, 0.9948 respectively. Therefore the reliability of the separator (that it won't be overfilled) is equal:

$$h = 0.9948 \cdot 0.9993 \cdot 0.9895 \cdot 0.9895 \cdot 0.9945 \cdot 0.9948$$

$$= 0.9630$$

$$g = 0.037$$

For upper failure rate with 90% interval, the failure rate of P_1 and P_6 = 3.16, P_2 = 3.62, P_3 and P_4 = 6.21 and P_5 = 3.20 and the probability that components will fail after 20 years are 0.6749, 0.5304, 0.3369, 0.3369, 0.5708, 0.6749 respectively. Therefore the reliability of the separator at year 20^{th} is equal:

$$h = 0.6749 \cdot 0.5304 \cdot 0.3369 \cdot 0.3369 \cdot 0.5708 \cdot 0.6749$$

$$= 0.0157$$

$$g = 0.9843$$

This is mean, the range between lower and mean reliability of the undesired event - occur after 20 years - can be varying between [0.037, 0.6684] and [0.6684, 0.9843] for mean unreliability and upper unreliability. It means without maintenance of the separator, there is very high probability – 98% - that the separator tank will over-fill at the beginning of year 21^{st}. We can use this reliability values to improve or redesign of the system. In this case it can be consider for another type of valve that more reliable, or redundancy of the system.

Additionally, a slightly change or slightly deviated in reliability value on a single component will also give a large effect on the final reliability value of the undesired event.

This is a simple example of the effect of uncertainty in data (described as U in risk description). The probability is only the value that analyse get from the history data or background knowledge information (described as K in risk description).

Another down-side of quantitative analysis is that it is nearly impossible to include probability value or any estimate for an error which cause by human since every single human has different way of doing things, different behavior, and different common sense.

Therefore we shall be aware when we using or describe the risk or the reliability of the system by probability or perform a quantitative analysis, due to the nature of uncertainties involved in the result.

Once we get a final evaluated value of the event, we can then design for system improvement, more safe efficiency, and more reliable system if needed. Redundancy of the system may be added to create more reliable of the system if it give more effective and efficiency to the system.

From paper OTC-7279[13] have not mention anything regarding uncertainty in data. The numbers and values used in calculation are directly from probability (P) and probability given background knowledge (P(A|K)) that we can be found from different sources that stated in the paper. For example OREDA which is the same data source that I selected to use in this paper. However the paper has mention that the data in OREDA is already include the error which caused by human, again as I state above it is nearly impossible to assign a concrete probability value for human error since every single person has different behavior and way of make things done.

From paper PSIG 0701[14] said:

> *"After the goals or undesired events have been defined and the data collected the analysis phase begins. The collected data is used to construct functional block diagrams for each system. A fault tree is then developed which will provide quantitative measures of risk and reliability."*

It is not necessary to construct Function Block Diagram in prior to construct a fault tree. However both diagrams can easily convert into one another in order to provide information of the system in a different view. Fault tree diagram give a better illustrate of event(s) that can trigger the undesired event while Function Block Diagram give a great overview of system, the flow of the system. We may use Function Block Diagram that we already have to double check whether we have missed any component which may lead to the failure of the system or the undesired event while we conduct a Fault Tree Analysis. On the other hand once we have a Fault Tree, we can analyse what can be add in order to improve reliability of the system by adding necessary redundancy to the system.

Reliability Block Diagram seems to be more profitable analysis that should be constructed in prior to Fault Tree analysis. It gives overview of the redundancy of the system, especially with cut-off approach. Cut-set analysis shows a combination of components that if they fail will cause the system failure and it can be convert as an example from Figure 6 Conversion of "OR" gate (FTA to RBD) and Figure 8 Conversion OF "and" GATE (FTA TO RBD).

The second part of the paragraph said "A fault tree is then developed which will provide quantitative measures of risk and reliability". As we discuss earlier in 3.2 that FTA can be conduct both quantitative and qualitative approach (see 3.2.1 Qualitative FTA and 3.2.2

Quantitative FTA). Fault tree can be used as Root Cause Analysis tool which does not need quantitative approach, qualitative will do the job well since the purpose of the analysis is to find what cause the failure.

On the other hand, if you use Fault Tree as a tool that gives support information in decision making process then quantitative approach is a must. We then can compare all alternatives we have, decide whether the design is good enough or safe enough or lower than ALARP. Those analyses need probabilistic numbers to judge and decide for the best alternative or solution. The important thing is to keep in mind at all time that probability is an uncertain number and ensure that it has been taking care of, has been reduce to as small as possible, has done additional analyse and the system is designed for the flexible of the uncertain numbers.

If the final frequency value or probability value is higher than the risk acceptance criteria, the system must be redesign. A redundancy of the system may be added and/or back-fitting for the operational system[15]

In additionally, the integration of FTA with other analysis method such as Bayesian Network Analysis or Event Tree Analysis or convert to Reliability Block Diagram is possible and should be done.

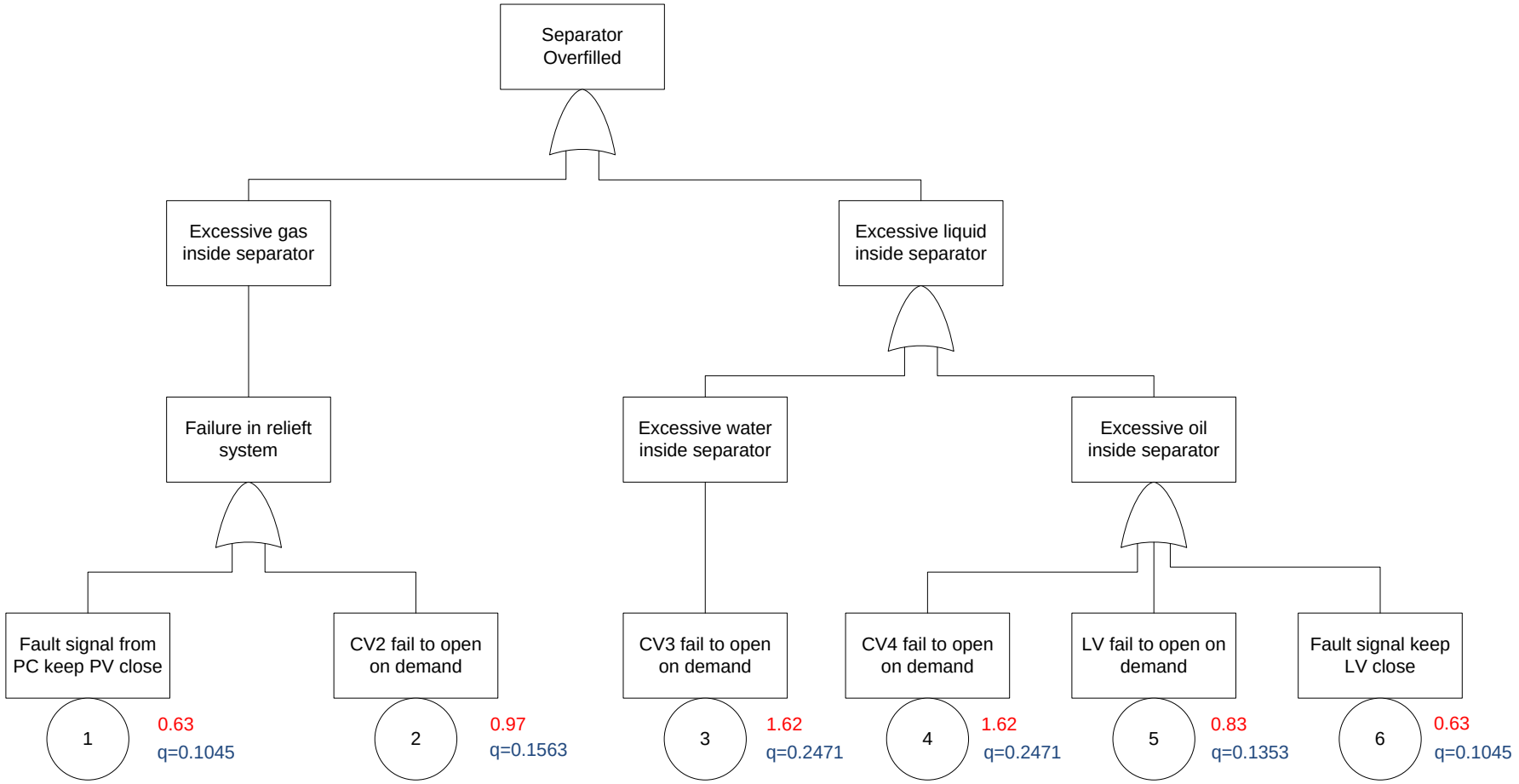


FIGURE 9 QUANTITATIVE FTA

3.2.3 Pros and Cons

Pros	Cons
➢ Can evaluate complex system ➢ Identify events that can cause "undesired event" ➢ Identify root causes ➢ Can use Boolean algebra or probability as additional analysis data ➢ Top-down analysis ➢ Can accommodate multi thread simultaneous ➢ Great tool for investigate accident, incident or anomaly ➢ Can accommodate human error in analyse ➢ Graphical and easy to understand ➢ Give a good overview of system's redundancy ➢ Possible for both quantitative and qualitative analysis ➢ Provide a logical framework for understanding the ways in which a system can fail	➢ Only include failure that cause the "top event" or "undesired event" ➢ Do not concern about effect of the failure ➢ Need to conduct analysis on each undesired event. It is time consuming if you have many events/failure that you need to analyse ➢ Easily to overlook at human factor during analyse ➢ Not able to analyse a degraded system (need to transform into reliability block diagram for future analysis) ➢ Require product/component expert to do the analyse ➢ Doesn't consider uncertainties

NB the data in the table above are from my own conclusion from many different papers and internet source I use. The two main sources are [16] and [17]

3.2.4 Weaknesses and Strengths

Weaknesses

Uncertainty – Due to the nature of data that always has uncertainty, we all know that certainty can only be achieved under strong experimental conditions, not in the real world and probability is just a tool used to express the uncertainties[11]. Therefore we must take those into account and do not uses the final result as a final answer for any decision we make base on the analysis we have done. Sensitivity analysis may conduct in order to examines the effect that the uncertainty has on the results[18]

Yue-Lung Cheng did a research on Uncertainties in Fault Tree Analysis[19] base on Guth's 3-value logic[20]. The theory has been taken False-Negatives and False-Positives into account and

generate into 3-value logic form. Guth has developed his theory based on Dempster-Shafer thory which then again came from two ideas. First is to obtain degrees of belief for one question from subjective probabilities for a related question and second is for combining such degrees of belief when they are based on independent items of evidence[21]. Further study of the theory is needed if the analysis would like to adapt this theory to reduce the uncertainty in data.

The theory and the idea of obtain an estimate probability from expert is great especially for an early phase of the project that involved in new technology and/or new hardware. But for a known project or a similar project as in the past, a combination or degree of belief from expert and history data seems to be less uncertain. Limbourg, Savic, Petersen and Kochs said in their paper that:

> *"Expert estimates can be merged, added and updated in a comprehensible way. Because of the conservative uncertainty treatment inherently included in DST, results could be further utilized, even in a skeptical environment. Experts have the possibility to describe critical uncertainties by intervals without the need to justify a distribution assumption. Therefore the method is especially useful in reliability and safety prediction during the first design stages [22]"*

Another way to treat the uncertainty is to perform a traditional way of FTA and perform an additional analysis method such as Bayesians Network, Bayesians update and Sensitivity Analysis which we will discuss later in Chapter 4. Dealing with uncertainties.

Do not concern about the effect of the failure – it only focus on what basic event could cause the failure, but does not give any information regarding the effect if those event actually occur either give any details how we should deal with those event. For further use, we can combine FTA and FMECA together. For example from the given example earlier in this chapter, once we analyse an undesired event by FTA and know that there is a possibility that the undesired event can occur. We then look into FMECA of those basic event in FTA such as "CV2 fail to open on demand". In FMECA we have listed all the possible failure, the effect of the failure on the subsystem, the effect of the failure on the system function, failure rate, detection of failure, criticality, and corrective action or risk reducing measure. Those will answer the question…when event A occurred and what's next?

Easy to overlook at human factor during the analysis – even though FTA is an analysis that support and cover human error, but it is often forgotten during the analysis. All activities that need a human in contribution of an operation must be considered as a treat that can trigger the failure. Probability value can be estimated and given according to the frequency and the duration

that one must work with the system. But as we all know that it is nearly impossible to give a good estimate for such value due to a unique behavior, habit of persons. Therefore the system should design for prevention of error caused by human as much as possible.

The human error can be reduced as minimum if we integrate proper risk reduction methods. There are many possible methods that can be integrated with the system to prevent human error, for example:

- Procedures and guideline on each operation must be available and provided in prior to field work. Worker must follow the procedures to avoid any incident or accident to occur. The guideline should include corrective actions when an undesired event occurs. In this case we can link FTA with FMECA report for a corrective action if the system fail due to a component failure
- All workers must pass a proper training session in prior to field work according to the responsibility he/she has to the system and the subsystem. Knowledge of the whole system is a plus, so that he/she will know the effect that can cause and what should it be done as he/she is part of the system itself
- Establish barriers to prevent errors. A common barrier such as warning message when worker trying to commit a fault input to the system, or when the system doesn't receive a proper input within the required period to a temporary barrier such as a barrier-rope to the area that a maintenance process is undergoing. Piper Alpha can give us a good example and lessons learn for human error
- Introduce educate program for workers. Toolbox talk is an example for such program, that allow and introduce workers to the equipments, tools, procedure, what are the DO and DON'T during the operation
- Good rotation and shift schedule should be established, due to human needs a good proportion of rest and relax and employer will get productivities in returned. A long working hours on the other hand gives tiresome and unproductive day for workers
- Reduce the need of human interaction in the system as much as possible, to avoid the error that cause by human. For an AI system it is possible to maintain and reprogram if the system is malfunction and it can be track, while human has many different way to perform a simple job

Not able to analyse a degrade system – in FTA system either fail or in function unless the undesired event in the analysis is given for example as fail when the system perform at 50%. A degrade system can be analyzed by transform FTA into a Reliability Block Diagram (won't be discuss in this paper). In that way we can analyse when a system given degrade performance and the end result of the whole system when one or more component are not fully function

Do not concern about the effect of the failure – due to the analysis is focus in what can trigger the failure but not the effect of the failure. In this case it is recommended that we combine FTA

with other analysis method such as FMECA which stated and show what the effect are and what recommended actions are when an incident occur

Strengths

Give a good overview of system's redundancy – can simply identify system whether it is lack of redundancy or overly redundant. This tool will be useful when the designer want to design for a higher reliable system. Since the redundancy will give higher availability to the system if the sub-system fails, make the system run consistency, safer for the personnel and environment. On the other hand, if the system is designed overly redundant, both CAPEX and OPEX will strongly increase (higher maintenance cost, higher expenses in purchase those extra components for the redundancy part). Designer need to make a decision base on the final reliability value that calculated from FTA, compare with the system without redundancy part whether it is worth to invest or not.

However, the different in two systems (with redundancy and without redundancy) give us two different final values, but nothing more. Who can decide whether 0.00009 differ in reliability give us a "green light" to start modify the system, when the effect in return maybe as small as 1 PLL in 10 year man hours but the company must invest 10 billion for the modification? This is one of the main problem that we facing when it comes to the safety of personnel.

No one can give a value of one life. Therefore it makes things more complicate when we would like to make a decision base on numbers only.

Can accommodate human error in analysis – this is an advantage of FTA in compare with FMECA. FMECA will only consider the possible failure of components without regard to external environment which actually play a big factor in risk analysis. However, human error is random event, cannot be predicted and nearly impossible to assign a concrete value for such an error. Therefore we will have to come back and think about uncertainty in data when we would like to give a probability value to a failure that cause by human

Provide an estimate time for maintenance purpose – Mean Time to Failure or Mean Time between Failures can be calculate and estimated by FTA. We can find information such as failure rate for each basic event, and MTTF is equal reciprocal of failure rate. Preventive maintenance is scheduled base on these values.

3.3 Hazard and Operability

Hazard and Operability (HAZOP) is a qualitative analysis technique that identifies potential hazards in a system and identify operability problems likely to lead to nonconforming product. HAZOP is based on a theory that assumes risk events are caused by deviations from design or operating intentions[23]. It can be described by using sets of "Guide-words" as a systematic list of deviation perspectives and "process parameters" as indicator of input or output of the process. It carried out by HAZOP team which composed of expert from many disciplinary who has no responsibility for the process and/or the performance of the analyzed system to avoid any bias to the task. The team brainstorming and give their opinion and suggestion regarding the node or topic that has been set in agenda.

The analyst examines plans, existing processes or operations in order to identify and evaluate problems that may represent risks to personnel, equipment, environment or prevent efficient operation[24]. Therefore the analysis should be doing when these document and information are available:

- P&ID (Process and Instrumentation Diagram)
- Process flow diagram
- Layout diagrams
- Material safety data sheets
- Provisional operating instructions
- Heat and material balances
- Equipment data sheets Start-up and emergency shut-down procedures

HAZOP is usually conducted during the design phase and construction period to ensure that recommendations, specifications and safety standard are met. Additionally for more efficiency and higher safety degree, HAZOP study can be conducted periodic and at every modification that affect the process to ensure that plant emergency and operation procedures are regularly reviewed and updated.

"Guide-words" according to IEC standard 61882:

> *"The identification of deviations from the design intent is achieved by a questioning process using predetermined "guide words". The role of the guide word is to stimulate imaginative thinking, to focus the study and elicit ideas and discussing"*

The basic set of relevant "Guide-words" to the operation must be selected and used for descript the deviation perspective. Examples of Guide-words are:

TABLE 4 BASIC HAZOP GUIDE-WORDS[4]

Guide-word	**Meaning**	**Example**
No (not, none)	None of the design intent is achieved	No flow when production is expected
More (more of, higher)	Quantitative increase in a parameter	Higher temperature than designed
Less (less of, lower)	Quantitative decrease in a parameter	Lower pressure than normal
As well as (more than)	An additional activity occurs	Other valves closed at the same time (logic fault or human error)
Part of	Only some of the design intention is achieved	Only part of the system is shut down
Reverse	Logical opposite of the design intention occurs	Back-flow when the system shuts down
Other than (other)	Complete substitution – another activity takes place	Liquids in the gas piping

Parameter are wording that descript input and output of the study node. Some example of parameters that can be found in oil and gas process facility and followed with an example:

- Temperature – more temperature → temperature is higher than expected in design limit
- Pressure – less pressure→ pressure is lower than normal
- Flow – no flow → blockage of the flowline
- Separation – reverse separation→ high volume (percentage) of hydrocarbon in water treatment system
- Speed – less speed → velocity of hydrocarbon from manifold to process facility is lower than expected
- Level – more level→ high level of water drop in gas outlet

3.3.1 HAZOP procedure[25]

1. Divide the operation process into study nodes. Define the scope of the node. We can separate the whole operation process into many small nodes by divide when a system undergoes a significant change. For example divided a separator system and a heat exchanger system into two nodes
2. Select a node that we want to study/analyse. The process engineer and others in the team who have knowledge of the system will explain the purpose of the node and determine the process safe limits. The team then discusses general questions about the scope and intent of the design base on the design information that we have available such as P&ID
3. Select relevant guide-words and parameter to the selected node. Determine the safety limit according to the design
4. Identify hazards and their causes with help of the selected guide-words and parameter. Keep in mind that HAZOP analysis is based on the believe that hazards in operation are caused from deviation that greater than the range in designed system (safety limit from no.3)
5. Identify and record causes and consequences (consequences to personnel, environment, economic) and suggest safeguard

> *"Safeguard is facilities that help to reduce the occurrence frequency of the deviation or to mitigate its consequences. There are five types of safeguard:*
>
> 1. *Identify the deviation*
> 2. *Compensate for the deviation*
> 3. *Prevent the deviation from occurring*
> 4. *Prevent further escalation of the deviation*
> 5. *Relieve the process from the hazardous deviation"*[4]

6. Repeat step 2 until all nodes analyzed

Figure 10 shows the diagram of HAZOP procedure. We may adapt and include more information such as the frequency of the deviation and analyse it as quantitative analysis. However, the frequency data are only the predicted value which has uncertainty in its.

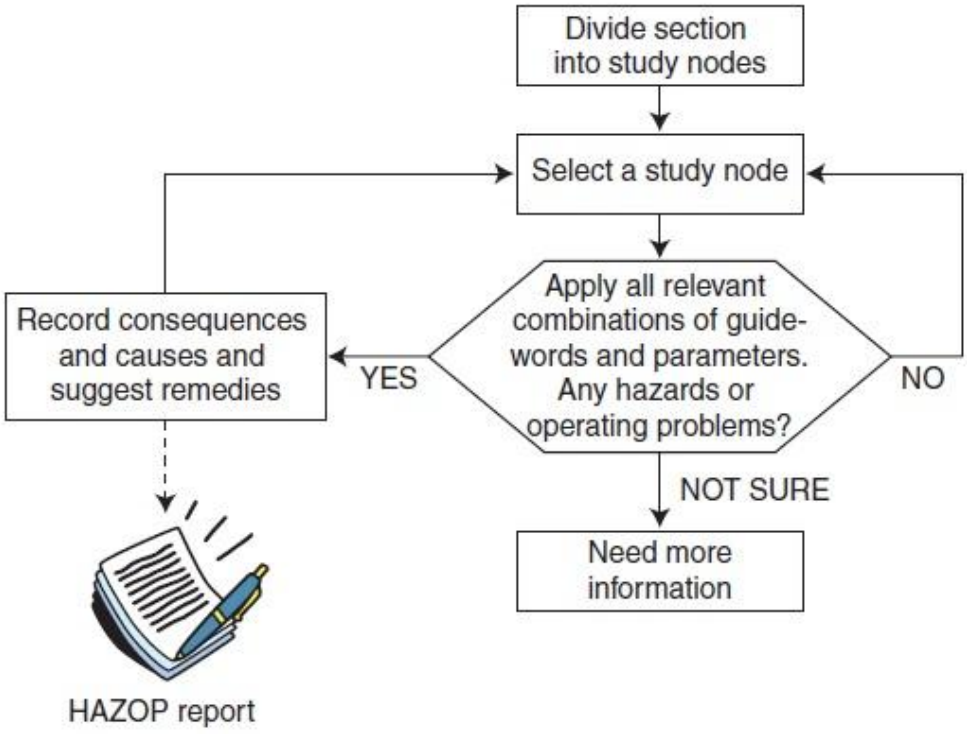


FIGURE 10 HAZOP PROCEDURE[25]

3.3.2 Pros and Cons

Pros	Cons
➢ Systematic examination[4] ➢ The team approach to a HAZOP makes it a multidisciplinary study[4] ➢ Utilizes operational experience[4] ➢ The process covers safety as well as operational aspects[4] ➢ Solutions to the problems identified may be indicated[4] ➢ Considers operational procedures[4] ➢ Covers human errors[4] ➢ Study led by independent person[4] ➢ Results are recorded[4] ➢ Accuracy of drawings and data used as a basic for the study[4]	➢ Time consuming[4] ➢ Focusing too much on solutions[4] ➢ Team members allowed to divert into endless discussions of details[4] ➢ A few of the team members dominate the discussion[4] ➢ The team may think system has "No problem" [4] ➢ The team may think this is "Waste of time" [4] ➢ Bias in team member "This is my design. This is my procedure and is the best."

➢ Experienced and skilled HAZOP team[4] ➢ Technical skills and insights of the team[4] ➢ Easily learned and performed by the operation team member ➢ Does not require considerable technical expertise for technique formulation ➢ No mathematic or statistic involve which mean less uncertainty ➢ Ability of the team to use the HAZOP approach as an aid to identify deviations, causes, and consequences[4] ➢ Ability of the team to maintain a sense of proportion, especially when assessing the severity of the potential consequences. [4] ➢ Brainstorming approach ➢ Cover all aspect from many different point of view of each profession ➢ Can use as a review of instrument and process design ➢ Hardly to be miss-analysis part of the system, since the analysis should follow from P&ID or other process diagram	

3.3.3 Weaknesses and strengths

Weaknesses

Time consume – the discussion may endless if the team discuss in too detail on the topic or on a single guide-word. Team leader play the main role to control and try to keep discussion within the focus topic and cut the unnecessary small details. The meeting shouldn't be longer than 2 hours per session

Discussion – the meeting will turn out useless if none of the team member dominates the idea during the discussion (everyone thought "no problem" or "the system is perfect"). As well as if only a few members dominate topics or idea regarding data in HAZOP report, the report and result of the meeting won't be as effective as it should. HAZOP will reach the most effective when the entire members share their knowledge, bring out the possible thought regarding safety and the possible deviation that can occur during operational mode. On the other hand, if team members go too deep in some detail and forget the agenda of the meeting, the discussion will also be useless as well

Bias – As the fact that human has bias. The team member may unfair in their decisions, they may get influenced by peoples and others opinions, rather than considering the facts. This will give a positive result for the analysis since the discussion may deviate from the actual system operation. Therefore, we should select a team member who has nothing to do with the system, not the designer, not the operator himself, not the project manager, not the electrical who work on the system, but someone that have knowledge and technical skill on those area and able to bring up some discussion regarding the system and hazard that may occur

Strengths

Cover human's error – the possible deviations are considered and identify the possible causes which included the deviation that can cause by human error

Brainstorming approach – great source of idea come from expert who has different backgrounds, independent and has no bias to the system. The team will speak out the possible deviation that can occur in the system base on the guide-words

Cover most of the operational hazard – once the team follows the guide-words and do the loop until all the guide-words and parameter have been analyzed. This can be proven that all possible hazards are considered and recorded

4. Dealing with uncertainties

The uncertainties are inherent in every activity. In everyday life we all facing uncertainty, we need to deal with it and make a decision. Things such as when we travel to somewhere we are "not sure" how to get there, we need to make a decision and take "chances". If we do a good research, we will reach to the destination without getting lost. Else we may end up in somewhere we may don't even know how to get home.

The same logic is also applied in oil and gas industry. In exploration phase, we never know what is under the ground or the seabed. We will need to do the research and gathering information to reduce the uncertainty of drilling and hit a dry well – in that case we will lose a fortune. There are many methods, tools or processes that we can conduct to reduce the uncertainty and they are vary by the project lift cycle and also vary by the objective of the operation.

During exploration phase to reduce the uncertainty of drill and hit a dry well, we may conduct a seismic study, coring a well, running a well-test analysis, consulting an expert, running logging surveys and learning from other fields, companies or peoples.

During design and planning phase to reduce the uncertainty of incident that can occur during operational period, we may conduct analysis methods such as FMECA, FTA and HAZOP as they already described under chapter 3. Analytical methods.

The questions are how can be combine those information with the observed data we already have, how much we willing to pay for such analysis and research, will the study assist us in decision making or change the decision, does the study worth its cost in compare with the reduction of the uncertainties.

There are two methods that are widely used in dealing with uncertainties. First is Bayesian Networks and secondly is Sensitivity analysis.

4.1 Bayesian networks

In the early way of calculate and estimate the probability is only base on past information data which has uncertainty in the value or "objective probability".

> "*Objective Probability or "Frequentist probability" is the probability that an event will occur based an analysis of the data from a large number of trials under the same condition, in which each measure is based on a recoded observation, rather than a subjective estimate."*

Sometime the same condition or the experimental cannot be repeated or perform an objective probability, therefore a "subjective probability" can give us a probability of the event to occur base on someone's "degree of belief".

> *"Subjective Probability a probability derived from an individual's personal judgment about how likely a particular event is to occur or "degree of belief". It is not based on any precise computation but is often a reasonable assessment by a knowledgeable person and from his/her past experience"*[26]

An example for subjective probability is a football commentator expert saying that Viking will defeat to Haugesund 1-0 before the game is actually started (if it already start it will turn from probability into fact). Means the commentator express "his degree of belief" based on his own experience of watching the game, knows the player, knows the tactic of the opinion, knows the manager and knows the factors of how to win the game. However others commentators may express their degree of beliefs in contrast depending on their individual states of knowledge. On the other hand, Viking and Haugesund play against each other in many matches in the past. Frequentist probability analyse will collect those data and calculate based on the past information of repeated game under the similar condition. However in this case it is hard since the teams may change the players, change the tactics, change the manager etc. Therefore there must be another way to combine these two types of probability to fix other weaknesses.

Another useful example of Subjective probability is when the repetition of the experiments is not possible. Objective probability is not possible to measure. The probability that we get in traditional way is Frequentist probability or Objective probability required a large number of trials that conduct under the same conditions and recorded the observe result then enter into statistic module in order to get probability of the event. An example of such case is Mr. A being hit by a car at the age of 30.

Bayesian networks allowed systematic way of combining knowledge – prior information – and data in order to eliminate those uncertainties from objective probability and update probabilities

when new evidence, new data – prior data – or new information becomes available. Prior information is the information that can obtain from expert judgment, technical knowledge, producer information, and data from similar cases in the past.

It is present in probability graphical model – Directed Acyclic Graph (DAG) – that shows the relationship between nodes and can be explained as the node which origin the arc is the "parent node" and the node where the arc is end is the "child node"

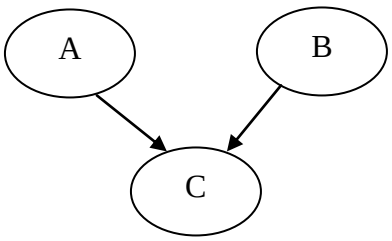


FIGURE 11 BASIC BAYESIAN NETWORKS

From Figure 11 nodes A and B represent "parent node" of node C "child node". It represents knowledge about an uncertain domain. Each node in the graph represents a random variable, while the edges between the nodes represent probabilistic dependencies among the corresponding random variables[27].

The diagram can be drawn backward (of arrow). We know the actual problem and list down what can cause the problem. The arc is point from parent node toward child node represent the possibility that the parent can cause what in child.

From the case study in this paper – separator overfills – we have analyzed the possible of component failure which can trigger the undesired event to occur by perform Fault Tree Analysis. After the analyst and system designer has study deeper into other possibility that could cause the undesired event, they found out that flow behavior can also be one of the reason that can cause overfill in the separator tank.

Slugging is one of the common problems in flow assurance for multiphase flow – simultaneous flow of gas and liquid – occurs in almost every aspect of the oil industry. Multiphase flow is present in the wellbore, flowlines and topsides processing facilities such as separator. Slug flow involves the intermittent production of liquid slugs and gas bubbles, some of which can be hundreds of meters long, and can lead to severe fluctuations in pressures and flow-rates throughout the production system if not properly predicted and managed[28].

Riser-based slugging is associated with the pipeline risers. Liquids accumulate at the bottom of the riser until sufficient pressure is generated behind it to push the liquids head over the top of

the riser, overcoming the static head. Behind this slug of liquid follows a slug of gas, until sufficient liquids have accumulated at the bottom to form a new liquid slug[28].

In this case study, we assumed that the expert studied and analyzed the flow behavior, and give a probability base on his degree of believe – subjective probability – that slugging will occur 24 slugs/hour[29] if no slug reduction mechanism has been installed or no proper predict and manage has been done. Those slug can cause overfill in the separator when a high volume of liquid slug filled up the tank. The results are poor separate result between gas and liquid hydrocarbon, equipment damage, unwanted flaring and etc.

Assumed that in one hour, 2 of 24 times riser-based slugging will cause overfilled in the separator and 1 out of 5 times that separator is not overfilled facing slug problem. Show in Table 5, Table 6 and Table 7 below.

TABLE 5 NUMBERS OF OBSERVATION

Overfilled	**Slugging**		**Total**
	Yes	**No**	
Yes	3	4	**7**
No	20	2	**22**
Total	**23**	**6**	**29**

TABLE 6 JOINT AND MARGINAL PROBABILITIES

Overfilled	**Slugging**		**Total**
	Yes	**No**	
Yes	0.10	0.14	**0.24**
No	0.69	0.07	**0.76**
Total	**0.79**	**0.21**	**1**

TABLE 7 CONDITIONAL PROBABILITIES FOR OVERFLOW AND SLUG

Overfilled	**Slugging**		**Total**
	Yes	**No**	
Yes	0.43	0.57	**1.0000**
No	0.91	0.09	**1.0000**

This is new information we obtained from a future study. Bayesian's formula enables and allows us to merge new information with the know data by following Bayesian's formula - Bayes' theorem is named after Thomas Bayes (1701-1761) who was an English Mathematician and Presbyterian minister. He never published what he found about this theorem himself, but the Bayes' theorem were edited and published after his death by Richard Price - Bayes' theorem:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

The theorem means probability of A given B as a condition of event A to happen. This theorem provides and explicit relation for the degree of belief accorded a hypothesis A, in light of evidence B.

From our case study, given S represent slugging and O represent overfilled. We wanted to find out the probability that the separator tank is overflow due to riser-base slugging or $P(O|S)$

$$P(O|S) = \frac{P(S|O)P(O)}{P(S)}$$

$$= \frac{0.43 \cdot 0.24}{0.79}$$

$$= 0.13$$

It means 13% of separator overfill can caused by slugging in another 87% is caused by the internal mechanism of the separator. However, the designer can reduce the total probability of separator overfill by reduce overfill that cause by slugging and overfill that cause by internal mechanism. To reduce P(O|S) we can add one more control choke valve or CV1 (See Figure 13 Separator process and instrumentation diagram) which open and close according to anti-slug algorithm – installed sensors along pipeline and interpret to control the choke valve.

4.2 Sensitivity Analysis

The decision or the final probabilities we get are based on the assumptions we made particularly with respect to uncertain quantities and variables over which we have choice. Sensitivity analysis showing how the numerical values depend on the assumptions made. It analyse under the idea of questions like "How accurately do we need to know these inputs?" "What extent the final decision is sensitive to changes in the inputs".

Steps to perform sensitivity analysis:

1. Select the input variable
2. Change the input variable one at the time. Changes of plus and minus 10% are often used
3. Recalculate probability after change input variable
4. A graph like tornado chart, spider chart or spider diagram can be used to illustrate the sensitivity of the input variable

From our case study, we found that 13% of separator overfilled can cause by slug under the assumption from observation we had that there are 24 slugs per hour. Again, we are still uncertain that there could be more or less than 3 out of 23 slugs that could cause the overfilled (since the size of slug is not stable, some are large and some are small) or there could be more than 24 slugs per hour or less. The changing of variable such as the number of slug we found in observation will affect the final probability value.

TABLE 8 SENSITIVITY ANALYSIS

Number of slug that cause overfill (out of 23 observed slug)	**0**	**1**	**2**	**3**	**4**	**5**	**6**
$P(O\|S) = \frac{P(S\|O)P(S)}{P(O)}$	0	0.0435	0.087	0.13	0.174	0.217	0.26

Since the number of slug that cause overfills is our input variable, is the one that contain uncertainty. We would like to perform the sensitivity analysis and see how the input variable can change the final probability. We will change from 0 to 6 (both plus and minus size from the original observed number). We then get the result in Table 8.

We can see that if the number of slug that cause separator overfill increased from 3 to 6 times out of 23 observed slug, will give 200% higher probability. That's mean the input value is very sensitive. We must look very careful when using this variable, when make any decision based on the information that calculated from this variable, to reduce the uncertainty or to implement a flexible solution to respond the outcomes of uncertain events.

Similar to the final probability with 90% interval that the separator is overfilled due to the failure of component(s) are between [0.037, 0.9843]. We can perform sensitivity analysis by change the failure rate on one of the component, such as "CV3 fail to open on demand" from 1.62 per 10^6 hours into 2.4 per 10^6 hours. Will the final probability that the undesired event to occur is still within the 90% interval? Can we ensure or confirm that 90% interval is good enough to represent the risk of the undesired event?

The case study I use in this paper may not look that it can cause a serious side effect or given a large consequences. Let's look at another example like the decision we need to make on firewall.

The firewalls are designed according to the design load and normally vary between section to section on the module. When an incident such as fire occur, the firewall provide module occupants time before the fire start to spread or cross from one section to another, occupants time to escape and firefighters a chance to save the module, offer a safe means of evacuation of a distressed module, . The resistant time is depending on the wall thickness and the design of the wall. For example 4 inches thickness firewall can tolerate 45 min fire rated, or 6 inches thickness wall can withstand 2 hours fire rated. However, we should design for a flexible and unexpected incident. After fire ignited, it may follow with a blast. Therefore, it is wise to perform the sensitivity analysis as a cross checking or double check the decision had made. Size of the fire, size of the module, size of the blast, pressure of the blast can be our input variable in the analysis when you analyse for PLL or AIR. We may compare all alternative we have with regard to expenses, value of the selection in return (how many more life can be safe from a different design), how likely the event going to happen and etc.

For a large and complex system, we may use computer software that have available in the market or create it in an excel sheet. A multiple change of input variables can be done at the time, but most were performed using an OAT (one-factor-at-a-time) approach. Each factor is perturbed in turn while keeping all other factors fixed at their nominal value. According to "Sensitivity Analysis Practices - Strategies for model-based inference" paper it is not wise to use OAT approach unless the model under analysis is proved to be linear[30].

5. Conclusion

Each analysis method provided information that assists in decision making regarding with design of the objective system (system in which we study). However a combination of method is a must in order to cover all aspect and in order to get all useful information needed to support decision making. FMECA give you an overview of all components in the system you analyzing, list of possible failure mode including suggest action when something go wrong with those component. FTA provided an easy illustration of what can cause an undesired event to occur and the probability of the event. All the possible hazard is listed by conducting HAZOP based on believe that hazard is caused by deviation from the design limit.

However, the information used during analysis is uncertain. Some based on history data, some based on repeated experimental are some are given from various source. Therefore Bayesian networks and Sensitivity analysis are there to reduce the uncertain of those analyzed data. Bayesian networks allow us to combine subjective probability with objective probability, expert knowledge with experimented data, new information with information you had from before, while Sensitivity analysis is to verify how sensitive the input parameter are to the analyzed data. Figure 12 show procedure diagram using in this paper.

In case the uncertain event occur, it would give big effect or big different from what we had analyzed. We must learn and know what uncertain information/data are and try to reduce or minimize it as much as possible. Since we cannot avoid the uncertain in data, therefore we must implement a flexible solution to respond the outcomes of uncertain events.

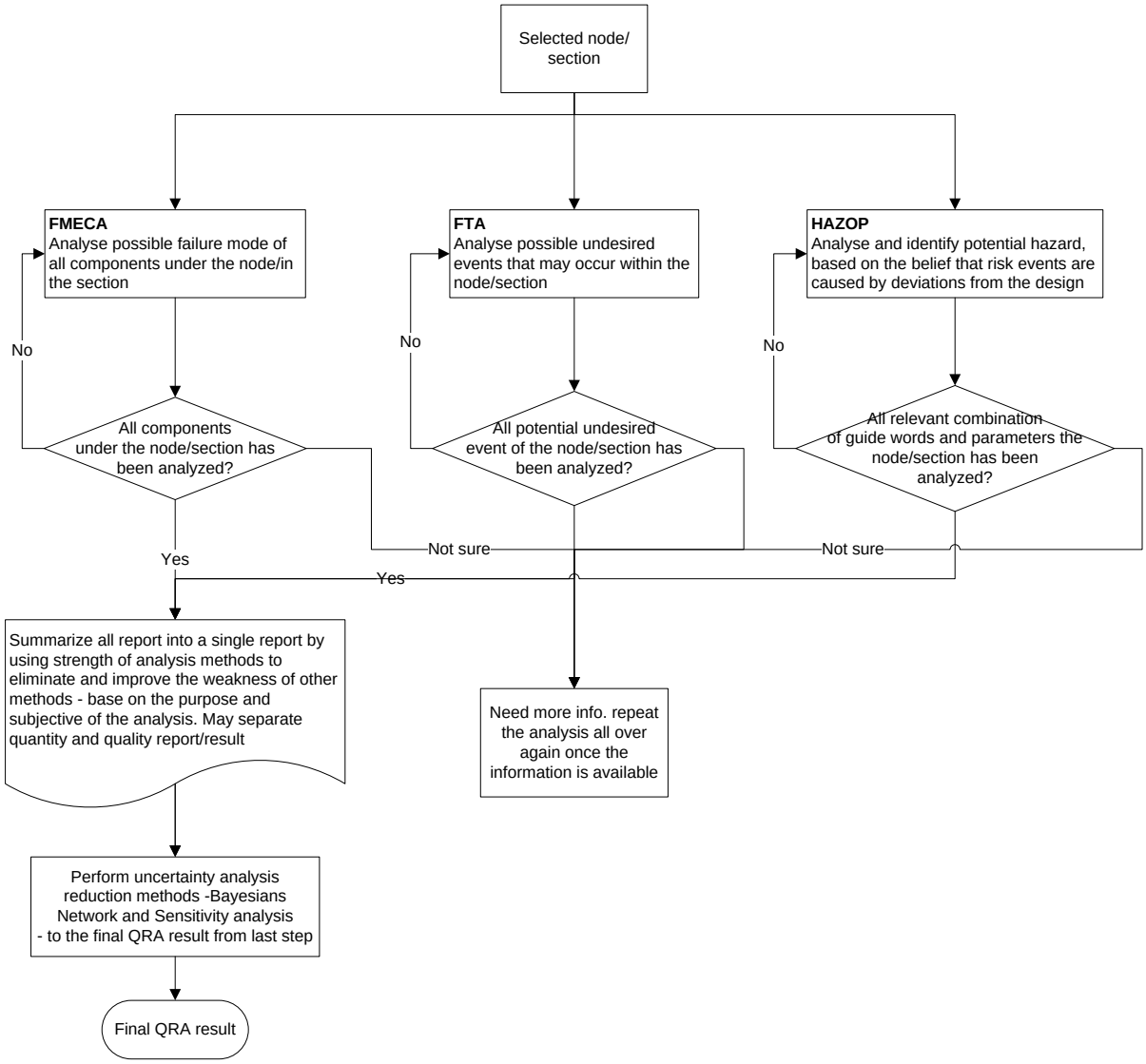


FIGURE 12 RISK ANALYSIS PROCEDURE USING IN THIS PAPER

6. References

1. Corporation, R. (2003) *Reliability Basics*.
2. NORSOK, *Criticality analysis for maintenance purposes*. 2001.
3. Aven, T., *Risk Analysis - Assessing Uncertainties Beyong Expected Values and Probabilities*. 2008: John Wiley & Sons, Ltd.
4. Rausand, M., *System Reliability Theory*. 2nd ed. 2004-5: Wiley.
5. SEMATECH, *Failure Mode and Effects Analysis (FMEA)*, in *A Guide for Continuous Improvement for the Semiconductor Equipment Industry*. 1992.
6. Netherland, F.W.H., *Use of Reliability Engineering Tools to Enhance Subsea System Reliability*, in *Offshore Technology Conference*. 2001, OTC: Houston, Texas.
7. Jervan, G. *Hazard Analysis*. Failure Modes and Effects Analysis - FMEA.
8. Rausand, M., *System Analysis, Failure Modes Effects and Criticality Analysis.* 2005(NTNU Lecture note).
9. B.Hebert, J.H., *Risk Minimization by the Use of Failure Mode Analysis in the Qualification of New Technology - Recent Project Experience in Completions and Sand Control*, in *Society of Petroleum Engineers*. 2005, SPE: Dallas, Texas.
10. Technology, T.I.o.E.a. (2010) *Quantified Risk Assessment Techniques - Part 1*. Failure Modes and Effects Analysis - FMEA.
11. Aven, T., *Misconceptions of Risk*. 2010: John Wiley & Sons Ltd.
12. Atkins, D.N.T. (2000) *Making Meteorological Measurement*. Uncertainty.
13. Roche, J.H.F.J.R., *System Safety Analysis of Well Control Equipment*, in *Offshore Technology Conference*. 1993, OTC: Houston, Texas.
14. Thomas Z.Moore, K.C.K., Klaus Brun, Alfredo Ramos-Aparicio, *Risk, Reliability, and Failure Mode Analysis*, in *Pipeline Simulation Interest Group*. 2007: Calgary, Alberta.
15. Burns, D.J., *Advanced Fault Tree Analysis in Offshore Applications*, in *Society of Petroleum Engineers*. 1991: The Hague, Netherland.
16. Safie, F., *An Overview of Quantitative Risk Assessment Method*, in *Technical Interchange Meeting*. 2000.
17. Amari, L.X.S.V., *Handbook of Performability Engineering*. 2008.
18. Security, H. (2010) *DHS Risk Lexicon*.
19. Cheng, Y.-L., *Uncertainties in Fault Tree Analysis*, in *Department of Information Management*. 2000, Husan Chuang College: Taiwan.
20. Guth, M.A.S., *A Probabilistic Foundation for Vagueness & Imprecision in Fault-Tree Analysis*. 1991, IEEE. p. 9.
21. Shafer, G. *Dempster-Shafer Theory*.
22. P. Limbourg, R.S., J. Petersen & H.-D. Kochs, *Fault tree analysis in an early design stage using the Dempster-Shafer theory of evidence*, in *Information Logistics*. 2007, University of Duisburg-Essen: Duisburg-Essen, Germany.
23. Institue, P.Q.R. *Risk Management Training Guides*.
24. Høyland, M.R.A., *System Reliability Theory*. Models, Statistical Methods, and Applications. 2004: John Wiley & sons.
25. Books, S.T., *HAZOP (Hazard and Operability Analysis)*. 2007-2012.
26. McColl, V.J.E.J.H. *Statistics Glossary*. Available from: http://www.stats.gla.ac.uk/steps/glossary/probability.html.
27. R., F.F.K., *Encyclopedia of Statistics in Quality & Reliability*. 2007, Wiley & Sons.
28. Janssen, E.F. (2011) *Flow Assurance*.

29. S.F.Kashou, N.E.B.a., *Slug Sizing/Slug Volume Prediction, State of the Art Review and Simulation*, in *Offshore Technology Conference*. 1995: Houston, Texas.
30. Andrea Saltelli, M.R., Stefano Tarantola and Francesca Campolong, *Sensitivity Analysis Practices. Strategies for Model-based Inference.* 2003.

7.Appendix

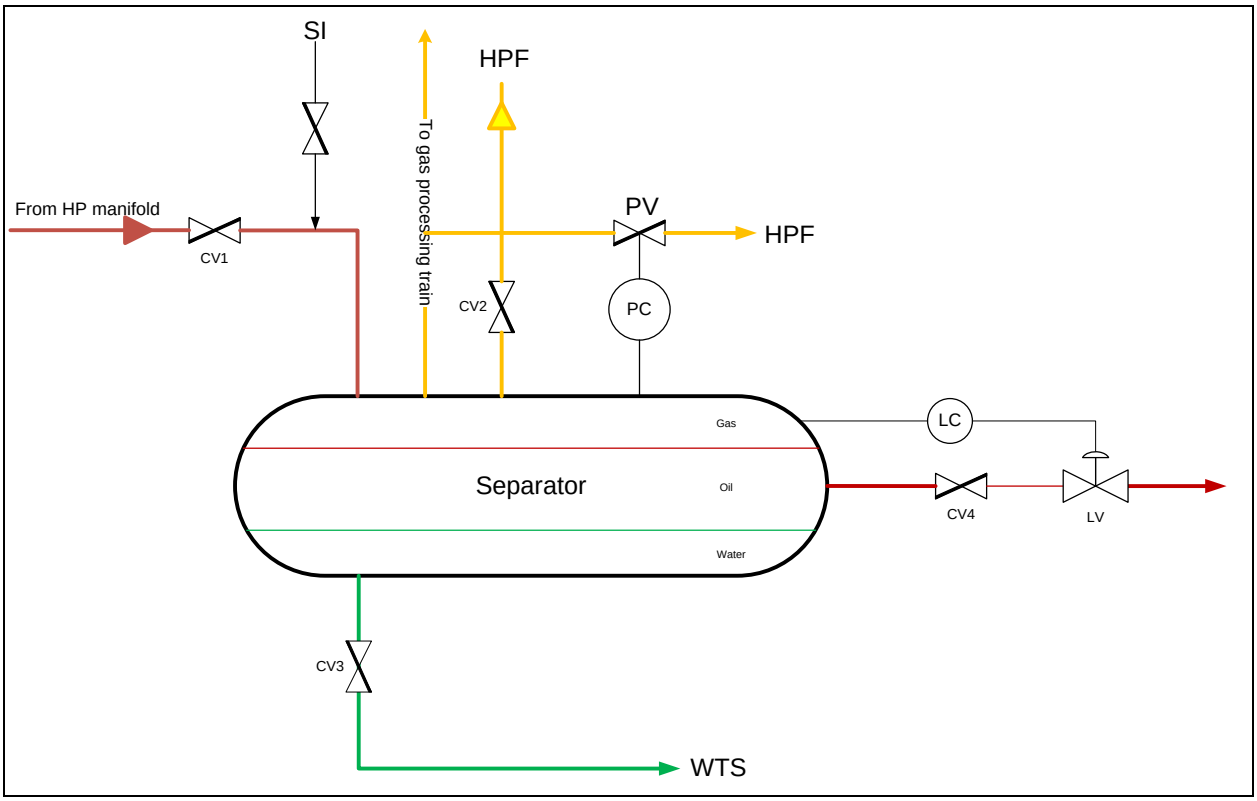


FIGURE 13 SEPARATOR PROCESS AND INSTRUMENTATION DIAGRAM